18. A method of modifying and distributing trust information, including the steps of:

providing a plurality of parties, said parties defining a hierarchy;

providing additional entities;

defining trust relationships by a party with other parties and, optionally, with at least one of said additional entities within parameters set by at least one higher party;

distributing trust information for said hierarchy from a top-level authority;

receiving said trust information by a client; and

validating said trust information by said client.

19. A method as in Claim 18, wherein said step of defining trust relationships by a party in said hierarchy comprises the steps of:

receiving a root certificate from any of a child in said hierarchy and an additional entity;

generating a fingerprint of said root certificate;

incorporating said fingerprint into a root security information object (RSIO), said RSIO including a root certificate of said party;

setting trust information for any of said child and said additional entity;

setting delegation information for any of said child and said additional entity; and

providing said RSIO to a parent in said hierarchy.

20. A method as in Claim 19, wherein said fingerprint comprises a digest of a signature in said root certificate.

21. A method as in Claim 19, wherein said step of defining trust information comprises the step of:

setting trust information for said child and said additional entity in a trust vector, said trust vector including a plurality of bits, wherein each bit designates a role.

22. A method as in Claim 19, wherein said step of setting delegation information comprises the step of;

setting delegation information for said child and said additional entity in a delegation vector, said delegation vector including a plurality of bits, wherein each bit designates a corresponding trust vector bit, said delegation information specifying whether said corresponding trust vector bit may be set by a party lower in the hierarchy.

B1 cont

23. A method as in Claim 19, wherein said step of distributing security information comprises the steps of:

linking said RSIO's to form a hierarchic security information object (HSIO); and

distributing said HSIO.

24. A method as in Claim 23, wherein said step of linking said RSIO's comprises:

matching a child's fingerprint in a parent's RSIO with the child's root certificate in the child's RSIO.

25. A method as in Claim 23, wherein said step of receiving said trust information comprises:

receiving said HSIO; and

receiving one of a root certificate and a chain of root certificates from said top-level authority.

26. A method as in Claim 23, wherein said step of validating said trust information comprises the steps of:

for each level of said hierarchy:

checking validity date of a child's RSIO in said HSIO;

validating a signature in said child's RSIO against a signature in said child's root certificate; and

checking that said child's fingerprint is contained in said parent's RSIO.

27. A method as in Claim 26, wherein said top-level authority's trust information is validated against said received root certificate or chain or root certificates.

28. A method as in Claim 18, further comprising the step of:

updating said trust information.

29. A computer program product for modifying and distributing trust information, said computer program product comprising a tangible medium having computer readable program code means embodied thereon, comprising computer readable program code for:

providing a plurality of parties, said parties defining a hierarchy;

providing additional entities;

defining trust relationships by a party with other parties and, optionally, with at least one of said additional entities within parameters set by at least one higher party

distributing trust information for said hierarchy from a top-level authority;

receiving said trust information by a client; and

validating said trust information by said client.

30. A computer program product as in Claim 29, wherein said computer program code for defining trust relationships by a party in said hierarchy comprises computer program code for:

receiving a root certificate from any of a child in said hierarchy and an additional entity;

generating a fingerprint of said root certificate;

incorporating said finger print into a root security information object (RSIO), said RSIO including a root certificate of said party;

setting trust information for any of said child and said additional entity;

setting delegation information for any of said child and said additional entity; and

providing said RSIO to a parent in said hierarchy.

31. A computer program product as in Claim 30, wherein said fingerprint comprises a digest of a signature in said root certificate.

32. A computer program product as in Claim 30, wherein said computer program code for defining trust information comprises computer program code for:

setting trust information for said child and said additional entity in a trust vector, said trust vector including a plurality of bits, wherein each bit designates a role.

33. A computer program product as in Claim 30, wherein said computer program code for setting delegation information comprises computer program code for;

B cont

setting delegation information for said child and said additional entity in a delegation vector, said delegation vector including a plurality of bits, wherein each bit designates a corresponding trust vector bit, said delegation information specifying whether said corresponding trust vector bit may be set by a party lower in the hierarchy.

34. A computer program product as in Claim 30, wherein said computer program code for distributing security information comprises computer program code for:

linking said RSIO's to form a hierarchic security information object (HSIO); and

distributing said HSIO.

35. A computer program product as in Claim 34, wherein said computer program code for linking said RSIO's comprises computer program code for:

matching a child's fingerprint in a parent's RSIO with the child's root certificate in the child's RSIO.

36. A computer program product as in Claim 34, wherein said computer program code for receiving said trust information comprises computer program code for:

receiving said HSIO; and

receiving one of a root certificate and a chain of root certificates from said top-level authority.

37. A computer program product as in Claim 34, wherein said computer program code for validating said trust information comprises computer program code for:

for each level of said hierarchy:

checking validity date of a child's RSIO in said HSIO;

validating a signature in said child's RSIO against a signature in said child's root certificate; and

checking that said child's fingerprint is contained in said parent's RSIO.

B1 cont

38. A computer program product as in Claim 37, wherein said top-level authority's trust information is validated against said received root certificate or chain or root certificates.

39. A computer program product as in Claim 29, further comprising computer program code for:

updating said trust information.

Please cancel Claims 1 – 17 from the application.